



Defense Information Systems Agency  
Joint Information & Engineering Office  
Center for Information Technology Standards  
<http://www-pki.itsi.disa.mil/>

12 July 2000

## Matrix of Target DOD PKI Requirements supported by Current Commercial PKI Standards

### Requirement Documents:

UR Department of Defense Public Key Infrastructure User Requirements, 29 February 2000

Requirement	Source	Supported by Standards	Reference	Notes
Supply public key certificates.				
Subscribers must have ability to check on the status and accuracy of the registration process.	UR: 3.2	No		
Certificates are to be formatted according to commercial standards, tailored by DoD specified certificate profiles.	UR: 1.3, 4.0.1	Yes	DoD Class 3 PKI Interface Spec.	
The PKI must supply certificates with lifetimes compliant with the DoD Certificate Policy (CP).	UR: 4.0.1	Y	DoD Class 3 PKI Interface Spec.	
Must be capable of supplying certificates with shorter lifetimes when required.	UR: 4.0.1	Y	RFC 2459: 4.1.2.5	RFC 2459 is being updated.
All certificates supplied by the PKI must be verifiable back to a trusted element known to the relying party.	UR: 4.0.1	Y	RFC 2459: 6	Certificate path validation. RFC 2459 is being updated.
Support multiple cryptographic algorithms and algorithm migration				
Must support a variety of public key cryptographic algorithms to create and certify public/private keys pairs.	UR: 4.0.1	Y	RFC 2437 RFC 2459: 7.3.1 DoD Class 3 PKI Interface Spec.	

Requirement	Source	Supported by Standards	Reference	Notes
Must support a variety of algorithms used to apply digital signatures (DS) to certificates and other PKI products.	UR: 4.0.1	Y	FIPS 180-1, RFC 2459: 7.2.1	SHA-1 with RSA Encryption will be used presently.
Must support the concurrent use of several digital signature algorithms for issuing certificates.	UR: 4.0.1	Y	RFC 2459: 4.1.1.2, 7.2	
Must be able to migrate over time to new signature algorithms.	UR: 4.0.1	Y	DoD Class 3 PKI Interface Spec.	Will migrate to ANSI X9.31 upon commercial acceptance.
<b>Provide key pairs and certificates for use with hardware cryptography</b>				
For each public key certificate the PKI produces, there is a corresponding private key.	UR: 4.0.1	Y	RFC 2510: 1.3 (13.), 2.3 RFC 2511: 4	
Key pairs may be generated centrally or locally, in software or in hardware.	UR: 4.0.1	Y	RFC 2510: 1.3 (6.), 2.2.1.3	
<b>Supply signature and encryption certificates</b>				
Must supply signature certificates, containing a public DS key that establishes the holder's identity or provides assurance of origin and integrity.	UR: 4.0.1	Y	RFC 2459: 4, 4.2.1.3, 7.2, 7.3 DoD Class 3 PKI Interface Spec.: 2.3	
Must supply encryption certificates, containing a public key used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.	UR: 4.0.1	Y	RFC 2459: 4, 4.2.1.3, 7.3 DoD Class 3 PKI Interface Spec.: 2.3.2	
Each individual public key certified by the PKI will be used for user identification and authentication (I&A), or for confidentiality key establishment, but not both.	UR: 4.0.1	Y	RFC 2459: 10 DoD Class 3 PKI Interface Spec.: 2.3	
All certificates contain information to identify the subscriber, and all certificates issued to each specific subscriber must contain the same identity information.	UR: 4.0.1	Y	RFC 2459: 4.1.2.6, 4.2.1.7 DoD Class 3 PKI Interface Spec.:	

Requirement	Source	Supported by Standards	Reference	Notes
			2.3	
Use of protocols (e.g., a Secure Socket Layer) that provide authenticated connections using encryption certificates are not prohibited.	UR: 4.0.1	Y	RFC 2165: App B RFC 2246: 7, D.3 RFC 2608: 9.2.2 DoD Class 3 PKI Interface Spec.: 2.2	

Program subscriber tokens				
Must program hardware tokens with public/private key pairs (or control the generation of key pairs by the token) and the corresponding public key certificates.	UR: 4.0.1			
Must support standardized delivery protocols so that it can program any token selected by the DoD.	UR: 4.0.1			
Must support remote programming of tokens.	UR: 4.0.1			
The LRA and the token must exchange information on certificates and protected private keys, and authentication data (e.g., PIN, password, biometric information) to support programming of tokens with public/private key pairs.	UR: 4.2			
The LRA and the token must exchange information on certificates and protected private keys, and authentication data (e.g., pin, password, biometric information) to support initialization for human subscribers.	UR: 4.2			

The CA and the token must exchange information on certificates and protected private keys, and authentication data to support programming of tokens with public/private key pairs.	UR: 4.2			
The CA and the token must exchange information on certificates and protected private keys, and authentication data to support	UR: 4.2			

Requirement	Source	Supported by Standards	Reference	Notes
initialization for human subscribers when LRA is not involved.				
<b>Securely distribute the PKI root certificate</b>				
Must have the means to securely distribute the trusted root's public key certificate to all subscribers and relying parties.	UR:4.0.1		DoD Policy & Procedure	
<b>Protect private keys</b>				
Must ensure that subscribers have control over the use of their private keys.	UR:4.0.1			
Must ensure that subscriber public keys are never exposed in plain text form.	UR:4.0.1			
On-line protocols for certificate and private key delivery.	UR: 3.2			
<b>Support user mobility</b>				
Must be able to use token and public/private key pairs with any DoD computer/platform, regardless of the operating system of the computer.	UR:4.0.1	Y		Standards as written either do not specify anything proprietary or technology specific, or cite non-proprietary alternates.
Must not impose any restrictions on the ability of multiple users to use the same platform or application.	UR:4.0.1	Y		Standards as written either do not specify anything proprietary or technology specific, or cite non-proprietary alternates.
<b>Establish legal policy for business use of digital signatures</b>				
Subscriber tokens must be able to create and verify digital signatures.	UR:4.0.1			
<b>Provide registration and renewal processes</b>				
The registration processes, and other certificate management processes, must support the	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
issuing and management of human subscriber certificates.				
The registration processes, and other certificate management processes, must support the issuing and management of device (e.g., web server, router, etc.) subscriber certificates.	UR:4.0.1			
Must ensure that each subscriber, of any type, is assigned a unique identifier that is both human usable and unambiguous to automated decision processes.	UR:4.0.1			
The registration processes must facilitate the request of such device subscriber certificates by the parties responsible for the device being registered.	UR:4.0.1			
CA and Supported Device must exchange certificates, protected private keys, and authentication data.	UR: 4.2			
Must provide processes for the renewal of certificates when they expire.	UR:4.0.1			
Must provide processes for the update of certificates' contents if the information changes.	UR:4.0.1			
Registration must be implemented in a simple and efficient manner such that it can be integrated into other, related, operational processes and supported by DoD organizations without requiring additional manpower.	UR:4.0.1			

PKI registration processes must be integrated with the operation of the Defense Enrollment Eligibility Reporting System (DEERS), and the Real-time Automated Personnel Identification System (RAPIDS).	UR:4.0.1			
Must provide procedural interfaces for supported applications functions.	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
Must provide procedural interfaces that can be used by supported systems to invoke and execute registration processes.	UR:4.0.1			
Must provide, where possible, technical interfaces that can be used by supported systems to invoke and execute registration processes.	UR:4.0.1			
LRA and CA must exchange registration information.	UR: 4.2			
LRA and CA must exchange information regarding new certificate requests.	UR: 4.2			
LRA and CA must exchange information for certificate renewal requests.	UR: 4.2			
LRA and CA must exchange information for certificate rekey requests.	UR: 4.2			
LRA and CA must exchange certificates.	UR: 4.2			
LRA and CA must exchange protected private keys.	UR: 4.2			
Provide revocation processes				
Must provide processes for certificate revocation prior to the end of their validity period.	UR:4.0.1			
LRAs must be able to request the revocation of a certificate on behalf of a PKI subscriber.	UR:4.0.1			
PKI subscribers must be able to directly request the revocation of their certificates without requiring the involvement of an LRA.	UR:4.0.1			
Must provide procedural interfaces that can be used by supported systems to invoke and execute revocation processes.	UR:4.0.1			
Must provide, where possible, technical interfaces that can be used by supported systems to invoke and execute revocation processes.	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
LRA and CA must exchange information for certificate revocation requests.	UR: 4.2			
<b>Recover from compromise</b>				
Must be able to recover from the compromise of private keys, including the private keys of human and device subscribers, and of PKI and infrastructure components such as CAs, RAs, and DSAs.	UR:4.0.1			
<b>Supply certificate revocation information</b>				
Must provide the capability to revoke a certificate (i.e., declare it invalid) prior to its expiration.	UR:4.0.1			
Must be able to revoke any individual subscriber certificate without affecting other certificates associated with that subscriber.	UR:4.0.1			
Must be able to revoke certificates issued to PKI elements such as CAs and LRAs.	UR:4.0.1			
Must make certificate revocation information widely available.	UR:4.0.1			
Supported applications must determine the validity of individual certificates before relying on them.	UR:4.0.1			
Must comply with the requirements of the DoD CP regarding CRLs.	UR:4.0.1		DoD CP	
Must generate and publish certificate revocations lists (CRLs), formatted according to X.509 and applicable profiles specified by the DOD.	UR:4.0.1			
CRLs are published via the directory system.	UR:4.0.1			
Supported applications must retrieve the published CRLs from the directory system.	UR:4.0.1			
Must publish CRLs in forms (e.g., a partitioned CRL) suitable for the constrained communications and directory access	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
capabilities of some supported applications.				
Must support alternative means for supported applications to check certificate validity via an on-line, interactive capability based on commercial standards such as the On-line Certificate Status Protocol (OCSP).	UR:4.0.1		Draft DoD OCSP Profile	
CA and On-line Status Responder must exchange information regarding certificate revocation.	UR: 4.2			
Supported application and On-line Status Responder must support the request for and response of certificate status information.	UR: 4.2			
<b>Provide key recovery services</b>				
Must provide for recovery of private confidentiality keys.	UR:4.0.1	Y	RFC 2510: 3.3.7, 3.3.8	RFC 2510 being updated.
Must be able prevent archiving of selected private keys (e.g., private keys from coalition partner forces).	UR:4.0.1	N		
Must not provide key recovery services for private digital signature keys, and must ensure the private signature keys are not archived or escrowed.	UR:4.0.1	N		
Must provide for two-party control over the stored key recovery information.	UR:4.0.1	N		
<b>Maintain an archive of PKI-generated security objects</b>				
Must establish and maintain an archive of the security objects generated (e.g., public key certificates, CRLs).	UR:4.0.1			
The storage of information in the PKI archive must meet the requirements of Records Management laws, rules and guidelines, and of the DoD CP.	UR:4.0.1		DoD CP	
Must provide a well-documented interface to enable supported applications to access, search, and retrieve objects.	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
<b>Generate trusted time stamps</b>				
Must provide a means of generating and returning to a supported application a trusted time stamp for a data object.	UR:4.0.1	N		X.509 does not define a time stamping service. An IETF standard is in development (ID: draft-ietf-pkix-time-stamp).
Must be an on-line service that can invoked on an as-needed basis.	UR:4.0.1	N		ID calls for the establishment of an on-line trusted Time Stamping Authority (TSA).
Must operate based on universal time.	UR:4.0.1	N		ID specifies the use of GeneralizedTime expressed in Greenwich Mean Time (Zulu).
Must be available to deployed units, including those that access the service via wireless communications networks.	UR:4.0.1	N		ID does not specify a wireless transport for TSA messages. MIME, FTP, socket, and HTTP mechanisms are defined.
Supported application and Time Stamp Service must support time stamp requests and responses.	UR: 4.2	N		ID specifies the request and response formats, and transaction steps taken on their receipt.
<b>Provide a digital notarization service</b>				
Must provide a digital notarization service that supported applications can use.	UR:4.0.1	N		X.509 does not define a digital notarization service. An IETF standard is in development (ID: draft-ietf-pkix-dcs).
Digital notarization service must be an on-line service that can be invoked on an as-needed basis by supported applications.	UR:4.0.1	N		ID calls for the establishment of an on-line trusted Data Validation Server (DVCS).
The notarization service must be available to deployed units, including those who must access the service via wireless communications networks.	UR:4.0.1	N		ID does not specify a wireless transport for DVCS protocol exchanges. MIME and HTTP/HTTPS mechanisms are defined.
The digital notarization service must provide supported applications and subscribers proof that the contents of a data object existed at a specific point-in-time and that the contents have not changed since that time.	UR:4.0.1	N		ID calls for the DVCS to generate Data Validation Certificates (DVC) which validates either the possession of data, the digital signatures on the data, or PK certificates at the time indicated in the DVC.
Supported application and Digital Notary Service	UR: 4.2	N		ID specifies the request and response

Requirement	Source	Supported by Standards	Reference	Notes
must support notarization requests and responses.				formats, and transaction steps taken on their receipt.
Provide a directory for dissemination of PKI-generated security objects				
PKI security objects must be generally available to supported applications on a DoD-wide basis.	UR:4.0.1			
Must provide a common directory service from which supported applications can retrieve public key certificates (for all subscribers: human users, network devices, and PKI components) and CRLs.	UR:4.0.1			
The PKI directory must segregate device certificates into a distinctive name space or segment of the directory information tree.	UR:4.0.1			
The PKI directory must store and permit retrieval of multiple certificates per subscriber.	UR:4.0.1			
The directory must provide access control and enforce identification and authentication of parties accessing the directory, as appropriate for the action(s) those parties are attempting to perform (e.g., read, search, add / update / delete content).	UR:4.0.1			
Access control must permit a service or agency operating elements to update other service or agency directory content in support of joint operations.	UR:4.0.1			
The PKI directory must be generally available and accessible from all classification domains.	UR:4.0.1			
The PKI directory must be generally available and accessible from temporary domains such as coalition networks during JTF missions.	UR:4.0.1			
To the maximum extent possible, the PKI directory requirement must be satisfied by the storage of PKI objects in available DII directory services.	UR:4.0.1			
The PKI directory must interoperate with all existing and planned local directory services.	UR:4.0.1			

Requirement	Source	Supported by Standards	Reference	Notes
The PKI must be capable of replicating information to all access points.	UR:4.1.5			
CA and DSA must exchange information necessary for posting of certificates.	UR: 4.2			
CA and DSA must exchange information necessary for posting of subscriber attributes.	UR: 4.2			
CA and DSA must exchange information necessary for posting of CRLs	UR: 4.2			
DSAs must exchange data synchronization data between themselves.	UR: 4.2			
LRA and DSA must exchange information necessary for directory information retrieval.	UR: 4.2			
LRA and DSA must exchange information necessary for posting of subscriber attributes.	UR: 4.2			
Supported application and DSA must support the request for and response of certificate information.	UR: 4.2			
Supported application and DSA must support the request for and response of CRL information.	UR: 4.2			
<b>Provide interoperability with other PKIs</b>				
Must support interoperability (e.g., by establishing cross-certifications) with other PKIs.	UR:4.0.1			
Must provide a means for subscribers certified under different PKIs to verify and thereby accept one another's certificates.	UR:4.0.1			
Must implement technical and policy controls on interoperability provisions to limit the risk assumed by the PKI and its subscribers to acceptable levels.	UR:4.0.1			
CA and other PKI must exchange information necessary for cross-certification.	UR: 4.2			

Requirement	Source	Supported by Standards	Reference	Notes
<b>Support community of interest separation and covert operatives</b>				
Public key certificates issued by the PKI must be usable to establish and maintain community of interest separation.	UR: 4.0.1			
Must be able to issue public key certificates for use by covert operatives while protecting the identity, organization, and position of such individuals from disclosure in unclassified channels.	UR: 4.0.1			
<b>Provide object signing certificates</b>				
Must provide certificates that can be used to verify digital signatures for source authentication and integrity protection of software objects.	UR: 4.0.1		X.509v4	
<b>Support enterprise-level access control</b>				
Attribute based control is needed to access the directory.	UR: 3.2			
Must support applications with products and services that aid in implementing enterprise level access control by providing an authenticated source of information about subscriber characteristics.	UR: 4.0.1			
Must generate attributes identifying subscriber privileges/permissions.	UR: 4.0.1			
These attribute definitions must be flexible to support role-based, clearance/privilege-based and other access control approaches.	UR: 4.0.1			
The attribute definitions must also support physical access control requirements as well as network-oriented access control requirements	UR: 4.0.1			
PKI must include attributes in subscriber public key certificates	UR: 4.0.1			
Must include attributes in attribute certificates	UR: 4.0.1			In general, public key certificates are more

Requirement	Source	Supported by Standards	Reference	Notes
linked to subscriber public key certificates				likely to be used to convey long-lived attributes such as citizenship, and attribute certificates are more likely to be used to convey short-lived attributes such as user roles within a particular supported application.
Must generate and distribute information (e.g., integrity-protected objects) specifying the interpretation of subscriber attributes	UR: 4.0.1			
Must provide means for appropriate authorities to request attributes and their inclusion in certificates and/or attribute certificates.	UR: 4.0.1			
Provide implementation aids.				
Toolkits and libraries must provide standard, tested, reusable implementations of PK-enabled security services.	UR: 4.0.1			

## NOTES:

## REFERENCES:

W3C REC-html32, HTML 3.2 Reference Specification

W3C REC-html401, HTML 4.01 Specification

RFC 1866, HyperText Markup Language 2.0

RFC 2109, HTTP State Management Mechanism

RFC 2227, Simple Hit-Metering and Usage-Limiting for HTTP

RFC 2518, HTTP Extensions for Distributed Authoring -- WEBDAV

RFC 2557, MIME Encapsulation of Aggregate Documents, such as HTML (MHTML).

RFC 2585, Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP.

RFC 2617, HTTP Authentication: Basic and Digest Access Authentication. (Obsoletes RFC 2069)

RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1 (Obsoletes RFC 2068)

X.509. Current DoD system is based on X.509v3, Jun 97. X.509v4 was approved for publication in April 00. DoD PKI system will migrate to v4 as industry does. X.509v4 is indicated where it specifically supports a requirement, otherwise v3 is assumed.